Remarks

Claims 1–5 and 21–31 are pending in this application. Claims 6–20 were cancelled in a previous amendment. Claim 1 is the only independent claim.

Prosecution was reopened on this application after an Appeal Brief was filed on 12/28/2006. All claims have been rejected on various grounds. Applicant has elected to amend claim 1 further to address the 35 U.S.C. § 112 issue.

Claim Rejections – 35 U.S.C. § 112

Claims 1–5 and 21–31 were rejected under 35 U.S.C. § 112, second paragraph, as being based on a disclosure that was not enabling, and as failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. In particular, the examiner asserted that claim 1 recites a "method of manufacturing devices" that was allegedly not enabled, as well as indefinite and unclear. The examiner stated that it was not clear how or if these devices are manufactured based on the claimed limitations because there were no steps related to manufacturing and were at most, according to the examiner, related to initializing a device.

The examiner further asserted that it was unclear how a key can be "stored within the device against the possibility of divulgement thereof by the device" because how a key can be stored without the device being able to divulge the key.

Claim 1 has been amended to clarify the aspects of the claim that the examiner asserted were unclear. Although the claim was believed enabled and clear, these amendments are made in an effort to address the examiner's points and further the prosecution, but not necessarily for patentability.

In particular, the claim preamble now relates to a method of providing devices that generate digital signatures (for use by third parties) rather than specifically reciting that the whole claimed method relates to manufacturing. The preamble of the claim has been further amended to recite that a device may be reliably and uniquely identified by a third party that receives an electronic message generated by a device and utilizes the electronic message in a message authentication. This is to emphasize the utility of the invention in connection with authentication schemes that are not strictly certificate authority based systems. Support for this amendment is found in the specification on page 2, lines 8–10 ("Message Authentication"), and

page 7, lines 26–30 ("...the message is authenticated ..."); page 20, line 29 through page 21, line 14; and other locations.

Further claim 1 now recites an initial step of manufacturing in a secure environment a device that generates a digital signature utilizing a private key of a public-private key pair. Support for a step of manufacturing in a secure environment is set forth in the specification on page 6, lines 33–36; page 19, lines 28–35 ("a secure manufacturing facility 102 ..."); page 20, lines 3–19 ("relevant manufacturing steps that are performed within the secure environment 114 are set forth in FIG. 2."); and other locations.

The claim has been still further amended to recited that the public-private key pair is generated while the device is still within the secure environment.

Further the claim has been amended to recite storing the key within the device utilizing security features to safeguard the private key against divulgement. Support for this amendment in particular is found in the specification on page 3, lines 26–37 through page 4, lines 1–28. A new dependent claim has been added to specify such security features (with support on page 3, lines 26–30) such as shielding, zeroization, auditing, tamper evidence and tamper response, etc.

Finally, the claim has been amended to recite the step of releasing the device from the secure environment for use in connection with generating a digitally signed electronic message that is provided by a user of the device to a third party that receives and authenticates the electronic message based on the public key and the other information. Support for this amendment is found at various places in the specification, in particular see FIG. 1 (device released into the world 106); specification page 20, line 20 through page 21, line 14.

With the foregoing amendments, it is believed that the claim is now fully in compliance with 35 U.S.C. § 112 – fully enabled by the specification, and also particularly pointing out and distinctly claiming the subject matter regarded as the invention.

Claim Rejections – 35 U.S.C. § 103

Claims 1–5, 21, and 25 were rejected under 35 U.S.C. 103(a) as being unpatentable over the *Fischer* patent (5,422,953) in view of the *Rosen* patent (5,557,518). As per claim 1, the examiner asserted that *Fischer* discloses a method having most of the features of claim 1 (which will not be repeated verbatim). The examiner acknowledged that *Fischer* fails to explicitly disclose that the device is manufactured in a secure environment and that the database is securely

linked within the secure environment. *Rosen* was cited as teaching manufacturing a device in a secure environment (citing to col. 11, lines 6–13) and a database containing linked information within a secure environment (citing to col. 10, lines 56–67 and FIG. 5). The examiner concluded it would have been obvious to a person of ordinary skill in the art to manufacture the device of *Fischer* in a secure environment and for the secure database to be within the secure environment. Motivation was found in *Rosen* col. 11, lines 6–13 and to provide trusted certificates to the trusted devices, citing to col. 10, lines 56–67 (emphasis supplied).

This rejection is respectfully traversed – for reasons including that shown in emphasis above, where it is amply clear that the motivation in *Rosen* is actually that of providing trusted certificates to trusted devices, not providing devices for use in message authentication as recited in claim 1.

It is urged that the examiner give proper appreciation to the significant and innovative aspects of the present invention, beyond ordinary innovation, that result from the use of an authentication model that does not require use of digital certificates – for which devices provided by the claimed method are intended. As has been repeatedly argued in this case, use of devices for message authentication, for example in connection with account based or account authority type authentication models, is notably different in many respects from certificate based authentication models such as *Rosen*.

Moreover, reliance on the *Fischer* patent as teaching a method for manufacturing devices that may be reliably and uniquely identified, especially the part about linking the public key with other information in a database, has already been argued in detail and will not be repeated. (See arguments "Appellant's Corrected Appeal Brief Pursuant to 37 C.F.R. §41.31" filed Dec. 28, 2006)("Corrected Appeal Brief"). The arguments and observations from that Corrected Appeal Brief are incorporated herein by reference and made a part hereof. All that the examiner has done in this rejection is substitute the *Rosen* patent for the *Spies* and/or *Ramasubramani* references. The *Rosen* patent does not supply the missing teachings, and does not rise to the level of a reference sufficient to deny applicant a patent on obviousness grounds.

In particular, *Rosen* is merely just another "certificate authority" type reference, although it is called an "identification authority" therein. See FIG. 5, identification authority network 202. "Identification authority networks 202 have authority servers 204 which manage a database of credentials and an authority transaction device 206 which issues and revalidates credentials."

Rosen, col. 10, lines 30–33. In other words, it is simply a certificate authority scheme by another name.

The examiner cited col. 10, lines 56–67 of *Rosen* as teaching that there is a database containing linked information within a secure environment. Note, however, that the cited portion of *Rosen* is describing the "primary trusted server 210", which has public keys stored in a primary trusted server public key PTS(PK) list. These are the keys of the trusted servers, not of the devices! The devices are those of the customer transaction device 188, which is the closest thing to the claimed devices as in this application.

Furthermore, note the purpose of the "primary trusted servers 210": "At the top of the hierarchy, and located at the Trusted Agency Network 208, are primary trusted servers 210 which certify and provide trusted server certificates (cert(TS)) to all the trusted servers 200 in the system." Rosen, col. 10, lines 51–55 (emphasis supplied). This is merely another certificate authority scheme. Such a scheme teaches away from method steps as now claimed. There is no certificate authority type scheme complicating the authentication using a device manufactured in accordance with claim 1, as amended.

How the examiner can rely on *Rosen* as providing a teaching of storing a public key and other information (as recited in the claim) in a secure database, for devices provided as in the claimed method, is nothing but a hindsight reconstruction – an attempt to find something in a reference that merely sounds applicable (a database that stores keys, that much which is admitted), without looking at the claims as a whole and what they relate to.

There is simply no evidence that *Rosen* teaches securely linking the recited other information with the public key of a device, after generation of the public-private key pair, but before releasing the device for use in connection with generating digitally signed messages, as recited. Rather, *Rosen* merely teaches storing public keys in a list of primary trusted server public keys (col. 10, line 60), which have nothing to do with the public keys of devices that are manufactured in the secure environment but not yet released for use. It is difficult to understand how the examiner can reasonably conclude that *Rosen* fills the gap in *Fischer*, which itself is a certificate authority type device and system, and is totally involved with certificate handling.

The citation to *Rosen*, col. 11, lines 6–13 only teaches manufacturing a device in a secure environment. But those things manufactured are the "trusted agents 120." Reading further in

col. 11 reveals the true nature of these "trusted agents" – they are used in a certificate authority scheme and are not the types of devices contemplated in the present invention:

> The trusted agent 120 generates the key pair and passes its public key (TA(PK)) to the requesting trusted server 200. The trusted server 200 incorporates this information and the TA(id) in to a trusted agent certificate cert(TA) and passes it back to the trusted agent 120 along with a PTS(PK) list, and an untrusted list. Finally the trusted agent 120 tests its newly received certificate and makes sure the certificate is valid.

Rosen, col. 11, lines 19–25 (emphasis supplied). In other words, again, this is a certificate authority scheme that does not involve associating device "other information" with the public key in the database in the secure environment, as now recited in claim 1, as amended. This does not teach, or motivate, or suggest, securely linking a public key with other information, in a database, in a secure environment, before releasing a device for use in message authentication. It only teaches generating a certificate for use in a complex certificate authority scheme involving certificate exchange.

For at least these reasons, there is not a *prima facie* case of obviousness, and applying the test of *Graham v. John Deere*, 383 U.S. 1 (1966)(which will not be repeated here), the differences between the claimed invention and the cited references is significant and beyond ordinary innovation, which is arguably now required under *KSR International Co. v. Teleflex, Inc.*, 550 U.S. ____, 127 S. Ct. 1727 (2007). The mere application of common sense to these cited references, without the hindsight benefit of applicants' many other patents in this area, would not lead a person skilled in the art to abandon the teachings of certificate authority type schemes to message authentication in the manner as set forth in claim 1, as amended.

It is therefore submitted that the rejection, even giving due weight to the obviousness analysis methodology of *KSR International Co. v. Teleflex, Inc.* and *Graham v. John Deere Co.*, is improper and should not be maintained.

Rejection of Dependent Claims

The dependent claims (2–5 and 21–31) were rejected as obvious on various grounds, typically a combination of the *Fischer* patent and *Rosen*, taken with *Ramasubramani*, *Schneier*, and *Menezes*, as regards specific claims.

Applicants have previously pointed out and argued the inapplicability of the *Ramasubramani*, *Schneier*, and *Menezes* references in the Corrected Appeal Brief. For the sake of brevity, those specific arguments and comments will not be repeated verbatim, but applicants incorporate such comments and arguments from the Corrected Appeal Brief as if the same were set forth fully herein. Applicants hereby reserve the right to argue separate patentability, if necessary (especially with regard to claims 4, 5, 22, 23, 24, 25, 27, 28, and 29). In this regard, the applicants submit and repeat the argument that these additional references fail to disclose, teach, suggest, motivate, or otherwise serve as a valid basis for an obviousness rejection of such dependent claims, as the applicants strongly believe that the references do not supply the teachings of those dependent claims.

Further, the doctrine of In re Fine, 837 F.2d 1071, 5 U.S.P.Q.2d 1596 (Fed. Cir. 1988) is applicable to these dependent claims – if an independent claim is nonobvious under 35 U.S.C. §103(a), then any claim depending there from is nonobvious. Accordingly, since claim 1 is nonobvious, it follows that the dependent claims are also nonobvious.

Double Patenting

Applicants note with appreciation the examiner's withdrawal of the obviousness type double patenting rejection based on application no. 10/248,629, now U.S. Patent No. 6,959,381. Although the applicants believe that with the foregoing amendments the claims of this application are patentably distinct, applicants nonetheless maintain the offer to submit a terminal disclaimer with respect to the three remaining patents on which an obviousness-type double patenting rejection was premised, namely U.S. Patent Nos. 6,892,302, 6,915,430, and 7,047,414.

Comment Regarding AADS v. CADS

The examiner noted at the conclusion of the office action (page 13) the applicants' attempts to overcome the previous rejections by distinguishing the account authority digital signature (AADS) authentication model as opposed to certificate authority digital signature (CADS) models. The examiner further noted that the claims did not reflect such statements.

In this regard the applicants respond as follows: claim 1 now recites a use of a device as provided by the claim in a message authentication, where a third party receives and authenticates an electronic message based on the public key of the device and the recited other information.

There is no certificate exchange or authority required or utilized in such a message authentication, which should be amply clear from the specification. It is believed that such amendments are sufficient to distinguish the claim from the strictly certificate based authentication models, where certificate exchange is required for various forms of authentication.

It should be understood that the claimed subject matter could itself be used as a component in a more complex certificate authority type scheme, but that is not a part of the claim. But it should be clear that the message authentication as claimed does not itself require certificates or certificate exchange in the claimed method or message authentication using the claimed subject matter. If further discussion of these aspects would be helpful, please contact the undersigned.

CONCLUSION

Accordingly, it is respectfully submitted that this application be allowed and that a Notice of Allowance be issued. If the Examiner believes that a telephone conference with the applicant's attorneys would be advantageous to the disposition of this case then the Examiner is encouraged to telephone the undersigned at 404–504–7720.

Respectfully submitted,

August 27, 2007

By: John R. Harris
Reg. No. 30,388

MORRIS, MANNING & MARTIN, LLP
3343 Peachtree Road, N.E.
1600 Atlanta Financial Center
Atlanta, Georgia 30326
(404) 233-7000
Email: jrh@mmmlaw.com
Docket No.: 10399–34384